Study and computation of a Hurwitz space and totally real PSL_2(F_8)-extensions of Q

Emmanuel Hallouin

Study and computation of a Hurwitz space and totally real $PSL_2(\mathbb{F}_8)$-extensions of $\mathbb{Q}$

Emmanuel Hallouin*

November 16, 2013

Summary. — Developing on works by Fried, Völklein, Matzat, Malle, Dèbes, Wewers, we give a method for computing a Hurwitz space and illustrate it on some example of number theoristic interest: we study and compute a family of degree 9 covers of $\mathbb{P}^1_{\mathbb{C}}$ with monodromy group $PSL_2(\mathbb{F}_8)$ and having four branch points. We deduce explicit regular $PSL_2(\mathbb{F}_8)$-extensions of the rational function field $\mathbb{Q}(\varphi)$ with totally real fibers. This gives rise to totally real polynomials over $\mathbb{Q}$ with Galois group $PSL_2(\mathbb{F}_8)$.

Contents

Introduction

This work deals with explicit inverse Galois theory. More precisely, let $\mathbf{G} = PSL_2(\mathbb{F}_8)$ acting on the nine points of $\mathbb{P}^1_{\mathbb{F}_8}$ and consider the two conjugacy classes $2a$ and $3a$ whose elements have cycle shapes $2^4 \times 1$ and 3^3 respectively. As suggested to us by Juergen Klueners, we study the family of degree 9 covers of $\mathbb{P}^1_{\mathbb{C}}$, with monodromy $\mathbf{G}$, ramified over four branch points and having the following branch cycle description:

$$\mathbf{C} = (2a, 2a, 2a, 3a).$$

By Riemann-Hurwitz formula, the total space of such a cover has genus 1.

Following works of numerous mathematicians like M.D.Fried, H.Völklein, B.H.Matzat, H.Malle, P.Dèbes, S.Wewers, we adopt the modular approach. Also we introduce the Hurwitz space that parameterizes our family.

*Groupe de Recherche en Informatique et Mathématique du Mirail (G.R.I.M.M.), University of Toulouse II, France.

Our computational point of view gives us the opportunity to illustrate some notions or phenomena turning around the general theory of Hurwitz spaces: let us mention the distinction between the *inner* and the *absolute* Hurwitz space, the problem of selecting totally real fibers, the braid action, the choice of a suitable curve on a Hurwitz space, the study of the boundary of a Hurwitz space, intersection theory on the universal curve, the patching and the deformation of a degenerate cover. Moreover, we show how explicit all this notions can be made. We organize the paper as follows.

Section 1 is devoted to the study of the Hurwitz spaces parameterizing this family. Because geometric and arithmetic Galois groups of covers in our family may differ, we both consider the *absolute* Hurwitz space and the *inner* one. As in [MM99], to find rational points on these varieties, we draw suitable curves on them. The "absolute" curve $\mathcal{H}$ and the "inner" one $\mathcal{H}_{\mathbf{G}}$, we have chosen, parameterize covers with a $\mathbb{Q}$-rational $3a$ type branch point and whose other three branch points are conjugate to each other. By means of braid action, we show that these curves are $\mathbb{Q}$-isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$. We end this section by introducing a pointed Hurwitz space used in the computation.

In section 2, we point out a specific degenerate cover in our family. Because its irreducible components are covers of $\mathbb{P}^1_{\mathbb{C}}$ with only three ramified branched points, we succeed in the computation of an algebraic model of this cover over $\mathbb{Q}$. Following methods of [Cou99], we then explicitly deform this degenerate element in order to compute an algebraic model of our family over $\mathbb{Q}((\pi))$ the completion of our pointed Hurwitz space at one point in its boundary. Comparing with our previous work in the area (see [HRD03]), this deformation step requires new algorithms since the genus of the total space is no longer zero but one.

In section 3, we both globalize and descend the previous local algebraic model, to deduce a global algebraic model defined over $\mathbb{Q}(\mathcal{H})$. The final result consists in a model of the universal family over $\mathbb{Q}(\mathcal{H})$ given with a degree 9 morphism to $\mathbb{P}^1_{\mathbb{Q}(\mathcal{H})}$ available from `http://www.univ-tlse2.fr/grimm/algo/hallouin/PSL_2_F_8.result`.

Even if the ramification data of the (degree 3) cover $\mathcal{H}_{\mathbf{G}} \to \mathcal{H}$ has been computed in section 1, we cannot compute the algebraic $\mathbb{Q}$-model of this cover at that time. Indeed, this computation requires arithmetic information from the algebraic model of the family. This is why we wait till section 4 to compute this cover.

Last, taking advantage of all the previous computations, in section 5, we give an example of an element of our family whose arithmetic and geometric Galois groups are equal to $PSL_2(\mathbb{F}_8)$ and which has an interval of totally real specializations. We end this work by giving two examples of totally real polynomials over $\mathbb{Q}$, one with Galois group equal to $PSL_2(\mathbb{F}_8)$, the other one with Galois group $P\Gamma L_2(\mathbb{F}_8)$. As far as we know, such polynomials had not been yet computed.

I would like to thank Jean-Marc Couveignes for having long discussions with me about this work during the (long and full of traps) computation and Pierre Dèbes for having read an early version of this paper.

1 Hurwitz spaces

1.1 Inner and absolute Hurwitz spaces

Moduli spaces parameterizing family of covers of $\mathbb{P}^1_{\mathbb{C}}$ are called Hurwitz spaces. They have been studied by Fried and Völklein in [FV91, Vl96]. We list here results we can deduce from this general theory.

We put a partial order on the four branched points by imposing that the last one has ramification type $3a$. This family is then parametrized by a quasi-projective regular variety over $\bar{\mathbb{Q}}$, called Hurwitz space, denoted $\mathcal{H}_3^1(\mathbf{G}, \mathbf{C})$ and which satisfies the following properties:

- Because of the transitivity of the braid action, this variety is absolutely irreducible.
- Since classes $2a$ and $3a$ are rational, $\mathcal{H}_3^1(\mathbf{G}, \mathbf{C})$ is defined over $\mathbb{Q}$.
- Let $\mathcal{U}_3^1$ denote the variety of partially ordered 4-tuple $(\{z_1, z_2, z_3\}, z_4)$ with $z_i \in \mathbb{P}^1_{\mathbb{C}}$ and $z_i \neq z_j$. The map:

$$\begin{array}{rccc} \mathrm{br}: & \mathcal{H}_3^1(\mathbf{G}, \mathbf{C}) & \longrightarrow & \mathcal{U}_3^1 \\ & h & \longmapsto & (\{z_1, z_2, z_3\}, z_4) \end{array}$$

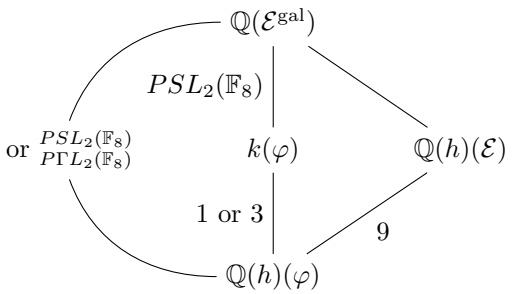
where z_1, z_2, z_3, z_4 are the four branched points (z_4 being the unique one with type $3a$) of the cover corresponding to h, is a finite étale morphism defined over $\mathbb{Q}$.

- Since $PSL_2(\mathbb{F}_8)$ is self-centralizing in S_9 the covers in our family do not have any non trivial automorphism. The moduli space is then a fine one. To each point $h \in \mathcal{H}$, there corresponds a degree 9 cover $\mathcal{E} \to \mathbb{P}^1_{\varphi}$ defined over $\mathbb{Q}(h)$, with *geometric Galois group* equal to $PSL_2(\mathbb{F}_8)$ and expected inertia.
- Since the normalizer of $PSL_2(\mathbb{F}_8)$ in S_9 is the semi-direct product of this group by the Frobenius:

$$P\Gamma L_2(\mathbb{F}_8) = PSL_2(\mathbb{F}_8) \rtimes \langle \mathrm{Fr} \rangle, \qquad \mathrm{Fr}((x:y)) = (x^2:y^2),$$

the *arithmetic Galois group* of the cover $\varphi : \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}(h)}$ may be bigger than the *geometric one*. In other terms, denoting by $\mathcal{E}^{\mathrm{gal}}$ the Galois closure of the cover $\mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}(h)}$, the constant field of $\mathbb{Q}(\mathcal{E}^{\mathrm{gal}})$ may be a cyclic degree

three extension k of $\mathbb{Q}(h)$ as shown in the following diagram:



The difference between the geometric and arithmetic Galois groups is also "parametrized". Let $\mathcal{H}_3^1(\mathbf{G},\mathbf{C})^{\mathrm{in}}$ denotes the quasi-projective regular variety over $\mathbb{Q}$ parameterizing the $\mathbf{G}$-cover with inertia $\mathbf{C}$. This is another Hurwitz space, often called *inner*, while the preceding one is called *absolute* (see [Fri95, FV91]). The inner Hurwitz space is also an absolutely irreducible variety and it is a covering of degree $\#|P\Gamma L_2(\mathbb{F}_8)/PSL_2(\mathbb{F}_8)| = 3$ of the absolute one. In our case, the cover is irreducible and cyclic of degree three:

$$\widehat{\mathrm{br}} : \mathcal{H}_3^1(\mathbf{G},\mathbf{C})^{\mathrm{in}} \to \mathcal{H}_3^1(\mathbf{G},\mathbf{C}).$$

With the above notation, if $\widehat{\mathrm{br}}(\hat{h}) = h$, then $k = \mathbb{Q}(\hat{h})$. So to any rational point $\hat{h}$ in $\mathcal{H}_3^1(\mathbf{G},\mathbf{C})^{\mathrm{in}}$, there corresponds a cover with geometric and arithmetic Galois groups equal to $PSL_2(\mathbb{F}_8)$. In the sequel, we will look for such a point such that the corresponding degree 9 cover of $\mathbb{P}^1_{\mathbb{Q}}$ has totally real fibers.

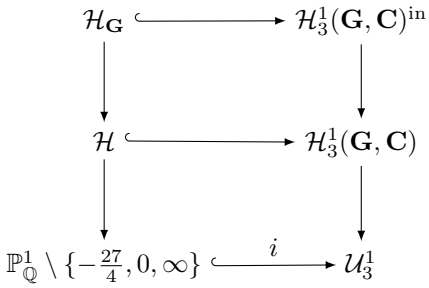
1.2 The good choice of a Hurwitz curve

1.2.1 The Hurwitz curve

In order to find rational points in these Hurwitz spaces, we follow [MM99] or more recently [Det04] and "draw rational curves on them": we choose to make the three ramification points with type $2a$ to be conjugate to each other. More precisely let i be the immersion defined by:

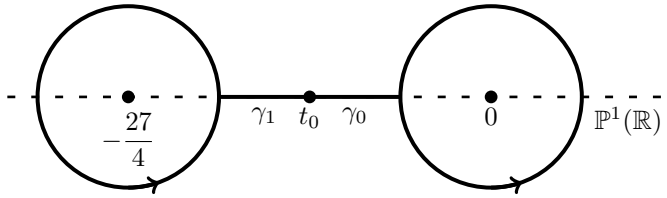
$$\begin{array}{ccc} i : \mathbb{P}^1_{\mathbb{Q}} \setminus \{-\frac{27}{4}, 0, \infty\} & \longrightarrow & \mathcal{U}_3^1 \\ t & \longmapsto & \left(\{\text{roots of } X^3 + t(X+1)\}, \infty\right). \end{array}$$

The curves we have drawn on our Hurwitz spaces come from the pull-back of this immersion:

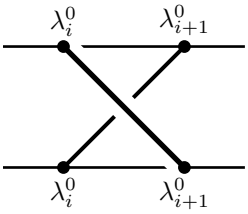


The left size in this diagram is a tower of covers of curves whose degree and ramification data can be computed using braid action. Before this, we need to recall some basic things about the π_1 of the bottom spaces.

Let us choose $t_0 \in \left]\frac{27}{4}, 0\right[$ and the following homotopic basis (or standard bouquet) of $\pi_1\left(\mathbb{P}^1 \setminus \{-\frac{27}{4}, 0, \infty\}, t_0\right)$



Put $i(t_0) = \left(\{\lambda_1^0, \lambda_2^0, \lambda_3^0\}, \lambda_4^0\right)$; regarding $\pi_1(\mathcal{U}_3^1, i(t_0))$, it is well known that it possesses a standard presentation in terms of the standard braids Q_i often drawn as follows:



These homotopic bases being fixed, we have:

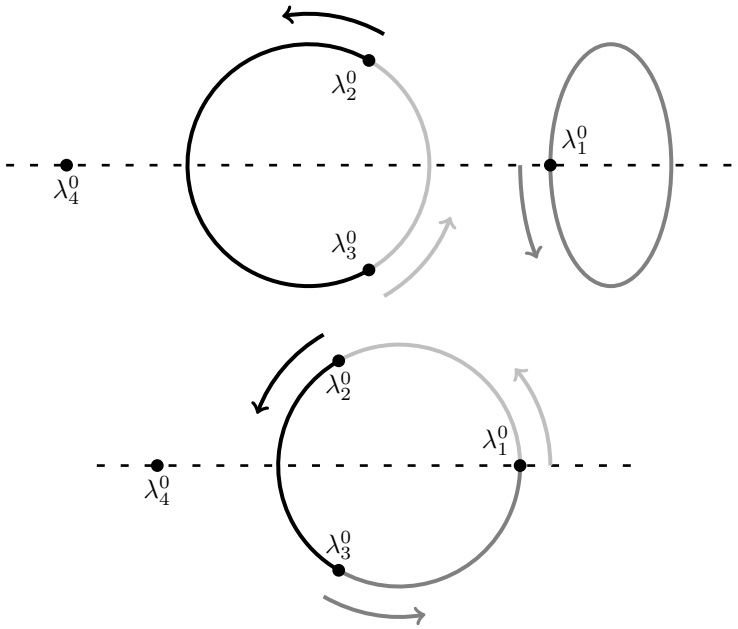
Lemma 1 *The map i_* induced by the immersion i on the π_1:*

$$i_* : \pi_1\left(\mathbb{P}^1 \setminus \{-\tfrac{27}{4}, 0, \infty\}, t_0\right) \to \pi_1\left(\mathcal{U}_3^1, i(t_0)\right).$$

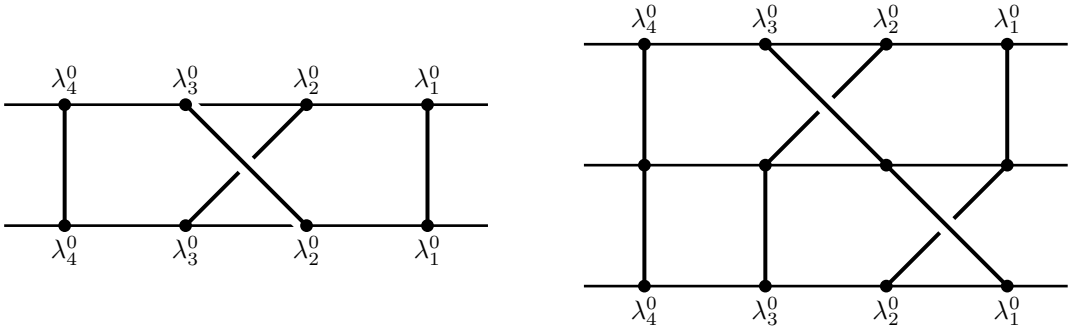
satisfies:

$$i_*(\gamma_1) = Q_2 \qquad \textit{and} \qquad i_*(\gamma_0) = Q_2 Q_1 \quad (\textit{first } Q_2 \textit{ then } Q_1)$$

Sketch of proof — In the two following pictures, we draw the images by i_* of the paths γ_1 and γ_0, that is the paths $i \circ \gamma_i$ on $\mathcal{U}_3^1$:



In the $\pi_1(\mathcal{U}_3^1, i(t_0))$, these two paths are respectively homotopic to the braids:



We recognize the braids Q_2 and $Q_2 Q_1$ respectively. □

Having carefully chosen an homotopic basis of $\pi_1\left(\mathbb{P}^1_{\mathbb{C}} \setminus i(t_0)\right)$, one can describe the fibers of $\mathcal{H} \to \mathbb{P}^1_{\mathbb{C},t}$ and $\mathcal{H}^{\text{in}} \to \mathbb{P}^1_{\mathbb{C},t}$ over t_0 by means of the Nielsen classes $\mathcal{N}(\mathbf{G}, \mathbf{C})^{\text{ab}}$ and $\mathcal{N}(\mathbf{G}, \mathbf{C})^{\text{in}}$ respectively. The ramification of the two preceding covers are then computed using the standard braid action formulas (see [FV91] or [Vl96]).

We summarize the results we can deduce from the computation of the braid action in the following proposition:

Proposition 2 *1. The curve $\mathcal{H}$ is irreducible, defined over $\mathbb{Q}$ and the cover $\mathcal{H} \to \mathbb{P}^1_{\mathbb{Q},t}$ is a degree 18 cover ramified over $t = -\frac{27}{4}, 0$ and ∞ with ramification type $9 \cdot 7 \cdot 2$, $3^5 \cdot 1^3$ and 2^9 respectively.*

2. The cover $\mathcal{H}_G \to \mathcal{H}$ is a cyclic degree 3 cover totally ramified at two of the unramified points of $\mathcal{H}$ above $t = 0$.

3. The curves $\mathcal{H}$ and $\mathcal{H}_G$ are genus zero curves and are $\mathbb{Q}$-isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$.

1.2.2 An algebraic model of the cover $\mathcal{H} \to \mathbb{P}^1_{\mathbb{Q}}$

In this section, we explain how we have computed an algebraic $\mathbb{Q}$-model of the degree 18 cover $\mathcal{H} \to \mathbb{P}^1_{\mathbb{Q}}$.

Proposition 3 *The degree 18 cover $\mathcal{H} \to \mathbb{P}^1_{\mathbb{Q}}$ is explicitly given by:*

$$t = H(T) = -\frac{27}{4}\frac{(T+3)\left(T^2+\frac{6}{49}T+\frac{9}{49}\right)\left(T^5-\frac{9}{49}T^4-\frac{3366}{2401}T^3+\frac{2430}{2401}T^2-\frac{2187}{2401}T+\frac{2187}{2401}\right)^3}{D(T)^2} \tag{1}$$

$$H(T)+\frac{27}{4} = -\frac{2^{28}3^{12}}{7^{14}}\frac{T^9(T-1)^2}{D(T)^2} \tag{2}$$

where polynomial D equals:

$$D(T) = T^9+\tfrac{9}{7}T^8-\tfrac{1188}{343}T^7+\tfrac{7668}{16807}T^6+\tfrac{188082}{823543}T^5+\tfrac{1246590}{823543}T^4-\tfrac{498636}{117649}T^3+\tfrac{2125764}{823543}T^2-\tfrac{531441}{823543}T+\tfrac{531441}{823543}.$$

Proof — Due to proposition 2, the cover $\mathcal{H} \to \mathbb{P}^1_{\mathbb{Q}}$ is a degree 18 cover ramified over three points with ramification type $(2^9, 3^5 \cdot 1^3, 9 \cdot 7 \cdot 2)$. Moreover, the two curves involved are $\mathbb{Q}$-isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ on which we can choose coordinates. Let t' be the coordinate on $\mathbb{P}^1_{\mathbb{Q}}$ such that $t' = 0, 1, \infty$ are the ramified points in the given order. Let T' be the coordinate on $\mathcal{H}$ such that $T' = \infty, 0, 1$ are the three points over $t' = \infty$ in the given order. There exist three unitary polynomials $P_0, P_1, Q_1 \in \mathbb{Q}[T']$, prime to each other, and $c \in \mathbb{Q}$ such that:

$$t' = \frac{P_0(T')^2}{cT'^7(T'-1)^2}, \quad t'-1 = \frac{P_1(T')^3Q_1(T')}{cT'^7(T'-1)^2} \quad \text{and} \quad \deg(P_0) = 9,\ \deg(P_1) = 5,\ \deg(Q_1) = 3.$$

By derivating equality $\frac{P_0^2}{cT'^7(T'-1)^2} - 1 = \frac{P_1^3Q_1}{cT'^7(T'-1)^2}$, we get:

$$P_0\left[2T'(T'-1)P_0' - P_0(9T'-7)\right] = P_1^2\left[(3P_1'Q_1+P_1Q_1')T'(T'-1) - P_1Q_1(9T'-7)\right]$$

and this leads to the system:

$$9P_1^2 = 2T'(T'-1)P_0' - P_0(9T'-7) \tag{3}$$

$$9P_0 = (3P_1'Q_1+P_1Q_1')T'(T'-1) - P_1Q_1(9T'-7) \tag{4}$$

Equation (3) gives ten relations between the coefficients of P_0 and P_1, all linear in the nine coefficients of P_0. We eliminate them and compute the degree 4 coefficient of P_1 with the unused equation. Then equation (4) gives nine relations between the coefficients of P_1 and Q_1 all linear in the four coefficients of Q_1. We eliminate them. The six unused equations relate the leaving four unknown coefficients of P_1. We solve this system using Groebner algorithms in `magma`. Constant c then equals to the leading coefficient of $P_0^2 - P_1^3Q_1$.

Last, changing the coordinates by putting $t = \frac{27(1-t')}{4t'}$ and $T = \frac{1}{T'}$ gives the expected model. □

Because of the automorphisms, we can not yet compute a $\mathbb{Q}$-model of the cover $\mathcal{H}_{\mathbf{G}} \to \mathcal{H}$. This will be done in section 4, at the end of this paper.

1.2.3 Labelling a few points and totally real fibers

In order to label a few points, let us describe precisely the elements in our family: to each value T_0 of the parameter T, there corresponds a cover:

$$\varphi : \mathcal{E}_{T_0} \xrightarrow{9} \mathbb{P}^1_{\mathbb{Q}(T_0)}, \qquad \text{genus}(\mathcal{E}_{T_0}) = 1.$$

(we use the same notation for the function φ and its specialization). The branch points of φ are ∞ and the roots of the polynomial:

$$(X-\lambda_1)(X-\lambda_2)(X-\lambda_3) = X^3 + H(T_0)(X+1)\ ;$$

the ramification fibers over these points are given by the following divisors equality:

$$\begin{aligned}(\varphi-\lambda_1) &= 2A+2B+2C+2D+E-(3L+3M+3N)\\ (\varphi-\lambda_2) &= 2G+2H+2I+2J+K-(3L+3M+3N)\\ (\varphi-\lambda_3) &= 2W+2X+2Y+2Z+U-(3L+3M+3N)\end{aligned}$$

where $A,B,C,D,E,G,H,I,J,K,L,M,N,U,W,X,Y,Z$ denote points on $\mathcal{E}_{T_0}$. Moreover, the constant field of $\mathbb{Q}(\mathcal{E}_{T_0}^{\mathrm{gal}})$ is $\mathbb{Q}(S_0)$ where $S_0 \in \mathbb{P}^1_{\mathbb{Q},S}$ satisfies $H_G(S_0)=T_0$.

The polynomial $X^3+t_0(X+1)$ is totally real if and only if $t_0 < -\frac{27}{4}$. In this case, one of its roots is greater than 3 and the other two, say $\lambda_2 > \lambda_3$, are negative. The real points of $H^{-1}\left(\left]-\infty,-\frac{27}{4}\right[\right)$ are the values $T_0 \in \mathbb{R}_+^* \setminus \{1\}$. Following criteria of [DF94] §2.3, one can prove that:

Proposition 4 *For every $T_0 \in \mathbb{R}_+^* \setminus \{1\}$, one has $t_0 = H(T_0) < -\frac{27}{4}$. All the roots of $X^3+t_0(X+1)$ are real; the singular values of the cover corresponding to $T=T_0$ are all real. Two of them, $\lambda_2 > \lambda_3$, are negative and $]\lambda_3,\lambda_2[$ is an interval of totally real specialization.*

1.3 Pointed Hurwitz space

In the sequel, we will need a scalar extension in order to rationalize the branch points. Instead of choosing the branch point of type $3a$ to be rational, we force two other branch points to be rational. Then we can suppose that the three branch points of type $2a$ are 0, 1 and λ^{-1} (∞ is still the branch point of type $3a$). This pointing involves an S_3-cover of $\mathcal{H}$ corresponding to the six ways to send the three roots of $X^3+t(X+1)$ to $\{0,1,\lambda^{-1}\}$ by an homography. To find the relation that rely t to λ, just start form the polynomial $X(X-1)(X-\lambda^{-1})$, kill the trace and make the constant and degree 1 terms being equal. This leads to the following:

$$t=-\frac{3^3(\lambda^2-\lambda+1)^2}{(\lambda-2)^2(\lambda+1)^2(2\lambda-1)^2}, \qquad t+\frac{27}{4}=-\frac{3^6\lambda^2(\lambda-1)^2}{2^2(\lambda-2)^2(\lambda+1)^2(2\lambda-1)^2}.$$

where $\mathcal{H}'$ denotes the pointed Hurwitz space we have introduce. This kind of Hurwitz space could also be studied by means of braid action. Nevertheless, since we only need to use this Hurwitz space locally, we can avoid this work. The point of $\mathcal{H}'$ we choose, is above $\lambda=0$ and $T=0$. Necessarily, the completion of $\mathcal{H}'$ at such a point gives rise to the following diagram of local fields, every extension being totally ramified: and where π is an uniformizing element of $\mathcal{H}'$ at the point we have chosen.

This pointing permits us to define ψ to be the homographic transformation of φ such that:

$$\begin{aligned}(\psi) &= (3L+3M+3N)-(2W+2X+2Y+2Z+U)\\ (\psi-1) &= 2G+2H+2I+2J+K-(2W+2X+2Y+2Z+U)\\ (\psi-\lambda) &= 2A+2B+2C+2D+E-(2W+2X+2Y+2Z+U).\end{aligned}$$

2 A degenerate cover and its deformation

We now focus on the degenerate cover corresponding to the value $T=0$ over $t=-\frac{27}{4}$ or locally at π over λ. We though investigate the boundary of our Hurwitz space. This boundary has been intensively studied by S.Wewers in his PhD thesis [Wew98].

In concrete terms, we want to compute an algebraic model of our family locally at π. This is an elliptic surface $\mathcal{E}$ over $\mathbb{Q}[[\pi]]$ whose special and generic fiber are respectively denoted by $\mathcal{E}_\pi$ and $\mathcal{E}_\eta$.

The key point is that the special fiber $\mathcal{E}_\pi$ of this surface can be explicitly described by mean of braid action as explained in [Cou99, Cou00].

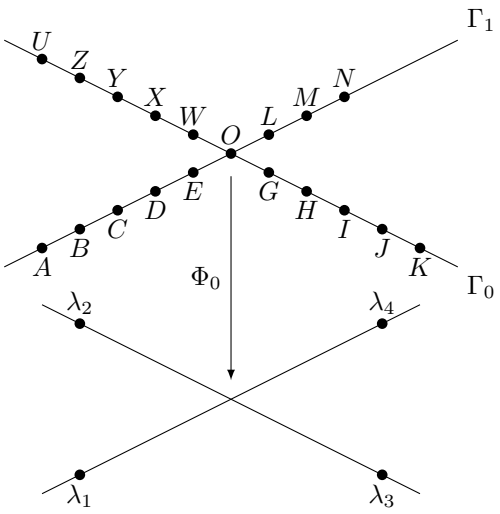
Indeed, degenerencies correspond to points coalescing and letting two branched points coalesce, one can compute the monodromy of the resulting degenerate cover. In our case, it is a cover of semi-stable curves with only two crossing components, meeting at a point denoted by O. The first one is a genus zero cover $\Gamma_0 \to \mathbb{P}_1$ with monodromy:

$$\begin{cases} \sigma_2 = (16)(28)(47)(59)(3) \\ \sigma_3 = (15)(27)(34)(89)(6) \\ \sigma_{1,4} = (165873429) \end{cases}$$

The second one $\Gamma_1 \to \mathbb{P}_1$ is an elliptic curve covering a $\mathbb{P}^1$ with monodromy:

$$\begin{cases} \sigma_1 = (14)(25)(67)(89)(3) \\ \sigma_{2,3} = (192437856) \\ \sigma_4 = (128)(346)(597) \end{cases}$$

Each component Γ_i corresponds to a discrete valuation v_i for $\mathbb{Q}(\mathcal{E})$.



Using intersection theory on the fibered surface $\mathcal{E}$ (see [Sil94], Chap III, §8 or [Liu02], §9.1), we are able to compute the valuations v_i of a function on $\mathcal{E}$ provide we know the horizontal part of its divisor. First of all, braid action shows that the thickness at the point O is 1. In other terms, the two components Γ_i of the special fiber $\mathcal{E}_\pi$ intersect with $\Gamma_0 \cdot \Gamma_1 = 1$ and we have $\Gamma_0 \cdot \Gamma_0 = \Gamma_1 \cdot \Gamma_1 = -1$.

Let us now compute the divisor of ψ on the surface $\mathcal{E}$: its horizontal part $(\psi)_H$ satisfies $(\psi)_H \cdot \Gamma_0 = -9$ therefore its vertical part $(\psi)_V$ is such that $(\psi)_V \cdot \Gamma_0 = 9$. Since $\psi(K) = 1$, necessarily $v_0(\psi) = 0$ and $(\psi)_V = a\Gamma_1$, $a \in \mathbb{Z}$. Intersection with Γ_0 shows that $a\Gamma_1 \cdot \Gamma_0 = a = 9$. In conclusion $(\psi)_V = 9\Gamma_1$ and ψ specializes to $\Gamma_0 \to \mathbb{P}^1$ while ψ/π^9 specializes to $\Gamma_1 \to \mathbb{P}^1$.

In conclusion the special fiber $\mathcal{E}_\pi$ is made of two components Γ_0 and Γ_1, both of them covering $\mathbb{P}^1$ by a degree 9 map. The component $\Gamma_0 \to \mathbb{P}^1$ is obtained by specializing the function ψ while the component $\Gamma_1 \to \mathbb{P}^1$ is obtained by specializing the function $\frac{\psi}{\lambda}$.

2.1 Algebraic model of the two components of the degenerate cover

The goal of this section is to compute independently an algebraic model of each component of the special fiber $\mathcal{E}_\pi$. This is easier than computing an algebraic model of a non degenerate cover of the family because each component is a degree nine cover of $\mathbb{P}^1_{\mathbb{C}}$ ramified at only three points (and not four).

• The component $\Gamma_0 \to \mathbb{P}^1$ of our degenerate cover is given by ψ_0 the specialization of ψ whose divisor satisfies:

$$(\psi_0) = 9O - (2W + 2X + 2Y + 2Z + U) \quad \text{and} \quad (\psi_0 - 1) = 2G + 2H + 2I + 2J + K - (2W + 2X + 2Y + 2Z + U).$$

This is a "Tchebycheff" like extension whose computation is easy (cf. § 2.2).

• On the other hand, the component $\Gamma_1 \to \mathbb{P}^1$ is given by ψ_1 the specialization of $\frac{\psi}{\lambda}$ whose divisor is given by:

$$(\psi_1) = 3L + 3M + 3N - 9O \quad \text{and} \quad (\psi_1 - 1) = 2A + 2B + 2C + 2D + E - 9O.$$

In this case, the computation of a model will be made easier by the fact that there is a 3-torsion point on Γ_1 (see the proof of the following proposition). This also explain that Γ_1 admits a Deuring normal form:

Proposition 5 *Let $\theta \in \bar{\mathbb{Q}}$ be a root of $\theta^3 - \frac{3375}{128} = 0$. The elliptic curve Γ_1 has the following Weierstrass equation $v^2+\theta uv+v-u^3 = 0$. Moreover in this model, the cover $\psi_1 : \Gamma_1 \to \mathbb{P}^1$ is given by the function $\psi_1 \in \mathbb{Q}(u, v)$ defined by $\psi_1 = \frac{32}{15}\theta + \frac{128}{225}\theta^2 u + \frac{v+1}{u}$.*

Proof — First we prove that the elliptic curve Γ_1 has a 3-torsion point. Let $d\omega_1$ denotes the holomorphic differential on Γ_1 and define the principal divisors (δ) by $\frac{d\psi_1}{d\omega_1}$ and (η) by $\frac{\delta^2}{\psi_1(\psi_1-1)}$. Then:

$$(\delta) = 2L + 2M + 2N + A + B + C + D - 10O, \quad (\eta) = L + M + N - E - 2O \Rightarrow \left(\frac{\psi_1}{\eta^3}\right) = 3E - 3O.$$

Choosing O as the origin of the elliptic curve Γ_1, the last equality shows that E is a 3-torsion point.

Secondly, elliptic curves with such a point have a generic model, known as the *Deuring normal form* (see [Sil86], Chap III, Exercise 3.23):

$$v^2 + auv + v - u^3 = 0, \qquad a \in \bar{\mathbb{Q}}.$$

The point $E = (0,0)$ is the marked 3-torsion point whose opposite $-E$ equals $(0,-1)$. Moreover, we have $(u) = E + (-E) - 2O$ and $(v) = 3E - 3O$.

We so have boiled down to the computation of the algebraic number a. To this end, we must take function ψ_1 into account; we note that $(\psi_1) = (v\eta^3)$ or $\psi_1 = v\eta^3$ by multiplying η by a suitable constant. It suffices to compute η; this function belongs to the dimension 3 vector space $\mathcal{L}(E+2O)$ of which $\{1, u, \frac{v+1}{u}\}$ is a basis. There exists $b, c, d \in \bar{\mathbb{Q}}$ such that $\eta = b + cu + d\frac{v+1}{u}$. Evaluation at E shows that $d^3 = 1$; we choose $d = 1$. The unknown constants a, b, c can be calculated observing the proportionality of the two functions:

$$v(\psi_1 - 1) \sim \frac{1}{\eta^4}\left(\frac{d\psi_1}{d\omega_1}\right)^2.$$

Differentiating the equality $\psi_1 = v\eta^3$ permits to write the right member in terms of u, v, a, b, c; rewriting the left one is easy. The result is that $b = 32/15a$, $c = 128/225a^2$ and $a^3 - 3375/128 = 0$. □

2.2 The first term of the algebraic model of $\mathcal{E}$

The two components of the special fiber $\mathcal{E}_\pi$ being computed separately, we now want to patch them in order to find an algebraic model of the special fiber $\mathcal{E}_\pi$. We pick two functions x and y in $\mathbb{Q}(\mathcal{E})$ and give heuristics about the equation between them. In the following "proof", some evidence for these heuristics to be true are developed; nevertheless only the success of the method at the end of §3 is a true proof.

Heuristic 6 *Let x and y be the two functions in $\mathbb{Q}(\mathcal{E})$ defined by their horizontal divisor and the following normalizations:*

$$\begin{cases}(x) = K + (-K) - 2L \\ x(U) = \pi,\end{cases} \qquad \textit{and} \qquad \begin{cases}(y) = K + U + (-K-U) - 3L \\ \frac{y}{x}(K) = \pi.\end{cases}$$

They are related by an equation with coefficients in $\mathbb{Q}((\pi))$ whose first order is given by:

$$(199 + O(\pi))\, y^2 + (5100 + O(\pi))\, xy + (1 + O(\pi))\, y + (10178 + O(\pi))\, x^3 + x^2 + \left(-\pi + O(\pi^2)\right) x = 0.$$

Moreover, the (x,y)-coordinates of the points $\{A, B, C, D, E, L, M, N\}$ can be computed; for example:

$$x(A) = 1017 + O(\pi), \qquad y(A) = 1264 + O(\pi).$$

"proof" — We need to make an hypothesis about the way of the sections $(-K)$ and $(-K-U)$ intersect $\mathcal{E}_\pi$: we suppose that we are in the "generic" situation, that is $(-K)\cdot\Gamma_1 = (-K-U)\cdot\Gamma_1 = 1$. In this case $(x)_H \cdot \Gamma_0 = 1$ and $(x)_V \cdot \Gamma_0 = -1$. Since $\frac{x}{\pi}(U) = 1$, there exists $b \in \mathbb{Z}$ such that $(\frac{x}{\pi})_V = b\Gamma_1$ and $(x)_V = (b+1)\Gamma_1 + \Gamma_0$. Intersecting with Γ_0 shows that $-1 = (b+1) - 1$, that is $(x)_V = \Gamma_0$. In exactly the same way, one verifies that $(y)_V = 2\Gamma_0$. Therefore functions x and y are parameters on Γ_1 and $\frac{x}{\pi}$, $\frac{y}{\pi^2}$ on Γ_0.

Functions x and y are related by a Weierstrass equation of type:

$$a_{02}y^2 + a_{11}xy + a_{01}y + a_{30}x^3 + x^2 + a_{10}x = 0,$$

where $a_{ij} \in \mathbb{Q}((\pi))$. The first significant term of the π-adic developments of these coefficients can be deduced from results of § 2.1.

• From the Γ_0 side, the function $\frac{x}{\pi}$ specializes to x_0 in such a way that $(x_0) = K - O$ and $x_0(U) = 1$. So x_0 is a parameter of the line Γ_0 and it is easily seen that:

$$\psi_0 = \frac{2}{1 + T_9\,(2x_0 - 1)}$$

where T_9 denotes the 9-th Tchebycheff polynomial.

The function $\frac{y}{\pi^2}$ specializes to the function y_0 such that $(y_0) = K + U - 2O$ and $\frac{y_0}{x_0}(K) = 1$. Therefore one has $y_0 + x_0^2 - x_0 = 0$. Since $\frac{x}{\pi}$ and $\frac{y}{\pi^2}$ are related by:

$$\pi^2 a_{02}\left(\frac{y}{\pi^2}\right)^2 + \pi a_{11}\left(\frac{x}{\pi}\right)\left(\frac{y}{\pi^2}\right) + a_{01}\left(\frac{y}{\pi^2}\right) + \pi a_{30}\left(\frac{x}{\pi}\right)^3 + \left(\frac{x}{\pi}\right)^2 + \frac{a_{10}}{\pi}\left(\frac{x}{\pi}\right) = 0,$$

we deduce that:

$$a_{01} = 1 + O(\pi), \quad \text{and} \quad a_{10} = -\pi + O(\pi^2).$$

We also deduce the first terms of the π-adic developments of the (x, y)-coordinates of the points $\{G, H, I, J, K, U, W, X, Y, Z\}$; for example one has:

$$x(G) = 8466\pi + O(\pi^2), \qquad y(G) = 7760\pi^2 + O(\pi^3).$$

For later use, we last compute the residue of ψ at $\frac{\pi}{x}$ and $\frac{\pi^2}{y}$; for example one has $\psi = -\frac{1}{2^{16}}\left(\frac{\pi}{x}\right)^9 + \cdots$.

• From the Γ_1 side, the functions x and y specialize to x_1 and y_1 such that:

$$\begin{cases} (x_1) = O + (-K) - 2L \\ (y_1) = 2O + (-K - U) - 3L \end{cases} \implies \begin{cases} x_1 \in \mathcal{L}(2L - O) \\ y_1 \in \mathcal{L}(3L - 2O). \end{cases}$$

Because, both of this two vector spaces have dimension one, with the help of `magma`, we are able to compute, up to a constant, x_1 and y_1 with respect to u and v. From the Γ_0 component, we remember that the residue of ψ at $\frac{\pi^9}{x}$ equals $-\frac{1}{2^{16}}$, therefore the residue of $\frac{\pi^9}{\psi}$ at x equals -2^{16}. The function x_1 is so the unique one such that $\psi_1^{-1} = -2^{16}x_1 + \cdots$. The equation that relates x_1 and y_1 is then easily computed:

$$199y_1^2 + 5100x_1y_1 + y_1 + 10178x_1^3 + x_1^2 = 0.$$

This permits to complete the first order of our model . □

2.3 The π-adic deformation

We now have to explicitly deform the preceding special fiber. In concrete terms, we want to compute the π-adic developments of all the preceding quantities. This step will require explicit computation in the algebraic group $\mathcal{E}_\eta$[1]. More precisely, we will need the:

2.3.1 The "line algorithm"

Let $E(x, y, z)$ be a cubic in $\mathbb{P}^2_{\mathbb{Q}((\pi))}$ and O a rational point on this cubic. The set of points is known to be endowed with a group law whose unit element is O. As this law will play a crucial role in the sequel, let us recall how it is defined. Given P, Q two points on E, we denote by $L_{P,Q}$ the line passing through P, Q and by $P * Q$ the third intersection points between E and $L_{P,Q}$ (Bezout theorem). Then the point $P + Q$ is the third intersection point between E and the line $L_{O,P*Q}$. Moreover, this group law operation can be easily computed.

So in $\mathbb{Q}((\pi))(E)$, one has:

$$\left(\frac{L_{P,Q}}{L_{P+Q,O}}\right) = P + Q - (P + Q) - O$$

The same way, if $P_1, \ldots, P_r$ are r points of E, then:

$$\left(\frac{L_{P_1,P_2}}{L_{P_1+P_2,O}} \times \frac{L_{P_1+P_2,P_3}}{L_{P_1+P_2+P_3,O}} \times \cdots \times \frac{L_{P_1+\cdots+P_{r-1},P_r}}{L_{P_1+\cdots+P_r,O}}\right) = P_1 + \cdots + P_r - (P_1 + \cdots + P_r) - (r-1)O.$$

Last, given $Z_1, \ldots, Z_r$ and $P_1, \ldots, P_r$ a family of points on E such that the divisor $\sum_i Z_i - \sum_j P_j$ is known to be principal, we are able to compute a function on E whose divisor is the preceding one.

Fact 7 *Given $Z_1, \ldots, Z_r$ and $P_1, \ldots, P_r$ a family of points on E such that the divisor $\sum_i Z_i - \sum_j P_j$ is known to be principal, say generated by a function f and let $\mathcal{F}$ be a family of points on E, then we are able to compute the values of f at all the points of $\mathcal{F}$ up to the **same** constant.*

2.3.2 The deformation

Let us return to the deformation. Knowing all the quantities modulo π^k, we complete all the π-adic developments by adding a generic unknown term: for example we put $x(A) = (\text{known terms}) + x_A\pi^k + O(\pi^{k+1})$ with $x_A \in \mathbb{Q}$ unknown to be found. Using the "line algorithm", we compute, modulo π^{k+1}, all the values:

$$\begin{cases} c_0\psi(p) & p \in \{A, B, C, D, E, G, H, I, J, K\}, \\ c_1(\psi - 1)(p) & p \in \{A, B, C, D, E, L, M, N\}, \\ c_2(\psi - \lambda)(p) & p \in \{G, H, I, J, K, L, M, N\}, \\ c_0\psi(P_i) & 1 \le i \le 30, \end{cases}$$

[1] If the genus of the generic fiber $\mathcal{E}_\eta$ would be greater than 2, this step would require computation in the jacobian of this curve.

where c_0, c_1, c_2 are unknown constants. We eliminate these constants using (for example) $c_0\psi(K)$, $c_1(\psi-1)(L)$ and $c_2(\psi-\lambda)(K)$ and deduce in term of all the π^k-terms, the values (modulo π^{k+1}) of the functions ψ, $\psi-1$ and $\psi-\lambda$. From them, we collect (linear!) equations in the unknown terms by writing that:

$$\begin{aligned}
\pi^9 &= \psi(A) = \psi(B) = \psi(C) = \psi(D) = \psi(E)\\
1 &= \psi(G) = \psi(H) = \psi(I) = \psi(J)\\
\pi^9 - 1 &= (\psi-1)(A) = (\psi-1)(B) = (\psi-1)(C) = (\psi-1)(D) = (\psi-1)(E)\\
-1 &= (\psi-1)(M) = (\psi-1)(N)\\
1-\pi^9 &= (\psi-\lambda)(G) = (\psi-\lambda)(H) = (\psi-\lambda)(I) = (\psi-\lambda)(J)\\
-\pi^9 &= (\psi-\lambda)(M) = (\psi-\lambda)(N)\\
1 &= \psi(P_i) - (\psi-1)(P_i)\\
\pi^9 &= \psi(P_i) - (\psi-\lambda)(P_i).
\end{aligned}$$

This deformation leads to the computation of a model of $\mathcal{E}_\eta$ over $\mathbb{Q}((\pi))$ the completion of $\mathbb{Q}(\mathcal{H}')$. We reach (and need) the precision $O(\pi^{376})$. For example, the equation coefficient:

$$a_{11} = 1 + 6778\pi + 700\pi^2 + 6801\pi^3 + 11005\pi^4 + \cdots + 4522\pi^{372} + 9470\pi^{373} + 10730\pi^{374} + 3650\pi^{375} + O(\pi^{376}).$$

We also know π-adic developments of the values of x and y at all the points $A, \ldots, Z$; for example:

$$\begin{aligned}
x(A) &= 1017 + 5644\pi + \cdots + 8350\pi^{374} + 6423\pi^{375} + O(\pi^{376})\\
y(A) &= 1264 + 1041\pi + \cdots + 10161\pi^{374} + 11201\pi^{375} + O(\pi^{376}).
\end{aligned}$$

Last it is easy to compute the π-adic development of the parameter T:

$$T = 1709\pi^2 + 8301\pi^6 + \cdots + 9535\pi^{374} + 5028\pi^{375} + O(\pi^{376}).$$

3 Computation of a rational model of the universal family

Since elements of our family do not have any non trivial automorphism, there exists a universal family (see [FV91], §4). The generic fiber is a genus one curve $\mathcal{E}$ defined over $\mathbb{Q}(\mathcal{H})$ with a degree 9 morphism $\varphi : \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}(\mathcal{H})}$ with monodromy group $\mathbf{G}$, ramified at the three roots of $X^3 + H(T)(X+1)$, ∞ and with expected inertia. The goal of this section is to compute an explicit model of this universal family.

3.1 A model of the total space $\mathcal{E}$ over $\mathbb{Q}(\mathcal{H})$

The curve $\mathcal{E}$ we are looking for and the generic fiber $\mathcal{E}_\eta$ of the elliptic surface we have computed in the preceding section are related by the following equality: $\mathcal{E}_\eta = \mathcal{E} \otimes_{\mathbb{Q}(\mathcal{H})} \mathbb{Q}((\pi))$ (that is why we both denote by $\mathcal{E}$ these two objects).

So the two functions x and y of §2.2 and 2.3 lead to a local algebraic model of $\mathcal{E}$ defined over the field $\mathbb{Q}((\pi))$ which is an extension of the completion of $\mathbb{Q}(\mathcal{H}) = \mathbb{Q}(T)$ at $T = 0$. Our problem is thus a descent problem. We first need to point out an algebraic model defined over $\mathbb{Q}(T)$ at least theoretically:

Lemma 8 *The curve $\mathcal{E}$ admits a total degree 3 model over $\mathbb{Q}(\mathcal{H})$: there exists two functions $f, g \in \mathbb{Q}(\mathcal{H})(\mathcal{E})$ that are related by an equation P of total degree 3 such that:*

$$P(f,g) = \sum_{i+j\le 3} b_{ij} f^i g^j = 0, \qquad b_{ij} \in \mathbb{Q}(\mathcal{H}).$$

Proof — Let $d\omega$ denotes the holomorphic differential on $\mathcal{E}$. The following divisor is rational over $\mathbb{Q}(\mathcal{H})$ and principal, say generated by $\Delta \in \mathbb{Q}(\mathcal{E})$:

$$(\Delta) = \frac{d\varphi}{d\omega} = A + B + C + D + G + H + I + J + W + X + Y + Z - 4(L + M + N)$$

This divisor helps to find a function f in $\mathbb{Q}(\mathcal{H})(\mathcal{E})$ with degree only equal to 3:

$$(f) = \left(\frac{\varphi^3 + H(T)(\varphi+1)}{\Delta^2}\right) = \left(\frac{(\varphi-\lambda_1)(\varphi-\lambda_2)(\varphi-\lambda_3)}{\Delta^2}\right) = E + K + U - (L + M + N)$$

We find another function of degree 3 by letting:

$$E' = K + U - E, \qquad K' = E + U - K, \quad \text{and} \quad U' = K + E - U.$$

Then the divisor $E' + K' + U' - (L + M + N)$ is rational over $\mathbb{Q}(\mathcal{H})$ and principal, say generated by g.

As $f, g \in \mathcal{L}(L + M + N)$ of dimension 3, they are related by a total degree 3 polynomial. □

We now explain how we have computed the equation P, i.e. the coefficients b_{ij} in term of T the parameter of $\mathcal{H}$.

The functions f and g are known up to a multiplicative constant: we normalize them by imposing that:

$$\left[\frac{b_{21}}{b_{30}} = \frac{b_{20}}{b_{30}} = -1\right] \Leftrightarrow [f(E') + f(K') + f(U') = h(L) + h(M) + h(N) = 1], \quad \text{where } h = \frac{f}{g}.$$

We also suppose that $b_{30} = 1$.

Looking at infinity, one gets:

$$h^3 - h^2 + b_{12}h + b_{03} = (h - h(L))(h - h(M))(h - h(N)) \quad \Rightarrow \quad \begin{cases} b_{03} = -h(L)h(M)h(N) \\ b_{12} = h(L)h(M) + h(L)h(N) + h(M)h(N). \end{cases}$$

The line algorithm permits to compute the π-adic developments of b_{03} and b_{12}. Finding an algebraic relation with T (of degree 1 in b_{03} and b_{12}) is then just a mater of linear algebra.

In exactly the same way, by evaluating equation P at points E', K' and U' (respectively E, K and U) one gets coefficients b_{00} and b_{10} (respectively b_{02} and b_{01}).

We need another family of rational points for the last coefficient b_{11}: we choose $P_1 = 2L - M$, $P_2 = 2M - N$ and $P_3 = 2N - L$. Always using the line algorithm, we compute the polynomials:

$$r(f) = \prod_{i=1}^{3}(f - f(P_i)) \qquad \text{and} \qquad s(f) = \sum_{i=1}^{3} g(P_i) \prod_{j \neq i} \frac{f - f(P_i)}{f(P_i) - f(P_j)}.$$

The last equation is nothing but $P(f, g) \equiv 0$ modulo $\langle r(f), g - s(f)\rangle$. This ends the computation of equation P. See proposition 9 for the complete result.

We could also compute the function $\varphi \in \mathbb{Q}(\mathcal{E})$ but it would require heavy precision in the π-adic developments (because of the height of the coefficients). We rather break off the computation on the universal family here; nevertheless, for each value T_0 of the parameter T, we will be able to compute the specialization of the function φ in the residual field $\mathbb{Q}(\mathcal{E}_{T_0})$ as we will see in the following section.

3.2 Computation of φ in $\mathbb{Q}(\mathcal{E}_{T_0})$

We need some notations to explain how to compute specializations of φ. To each family $\mathcal{F}$ of points on $\mathcal{E}$, and each $1 \leq i \leq \#\mathcal{F}$, we denote by $\sigma_{\mathcal{F},i} : \mathbb{Q}(\mathcal{H})(\mathcal{E}) \to \mathbb{Q}(\mathcal{H})$ the i-th symmetric polynomial in the values at the points of $\mathcal{F}$; for example, if $\mathcal{F} = \{E, K, U\}$, one has:

$$\sigma_{\mathcal{F},1}(\varphi) = \varphi(E) + \varphi(K) + \varphi(U) \quad \sigma_{\mathcal{F},2}(\varphi) = \varphi(E)\varphi(K) + \varphi(E)\varphi(U) + \varphi(K)\varphi(U) \quad \sigma_{\mathcal{F},3}(\varphi) = \varphi(E)\varphi(K)\varphi(U).$$

We now fix T_0 a value of the parameter T. Just putting T equal to T_0 in the equation P computed in §3.1, one gets an equation for the curve $\mathcal{E}_{T_0}$ (see §5 for an example). More precisely, in the function field $\mathbb{Q}(\mathcal{E}_{T_0}) = \mathbb{Q}(f, g)$, we have:

$$(f) = K + E + U - (L + M + N) \qquad (g) = K' + E' + U' - (L + M + N).$$

The function φ we are looking for satisfies $\varphi \in \mathcal{L}(3L+3M+3N)$ which is spanned by the functions $(f^i g^j)_{0 \leq i+j \leq 3}$. So computing φ reduce to find nine constants $c_{ij} \in \mathbb{Q}(T_0)$ such that:

$$\varphi = \sum_{0 \leq i+j \leq 3} c_{ij} f^i g^j.$$

First, the knowledge of the zeros E, K, U of f permits to obtain three easy equations: indeed $\varphi(E), \varphi(K), \varphi(U)$ are the roots of $X^3 + H(T_0)(X + 1)$ and one must have:

$$\sigma_{\{E,K,U\},1}(\varphi) = 0, \quad \sigma_{\{E,K,U\},2}(\varphi) = -\sigma_{\{E,K,U\},3}(\varphi) = H(T_0)$$

Secondly, in terms of divisors, one has:

$$2\left(\frac{d\varphi}{d\omega}\right) = \left(\frac{\varphi^3 + H(T_0)(\varphi + 1)}{f}\right) = 2(A + B + C + D + G + H + I + J + W + X + Y + Z) - 8(L + M + N)$$

We evaluate the two functions above at few points to obtain new equations.

Two other easy equations come from the fact that the values of these two functions at E', K', U' (the zeros of g) are proportional. The rest of the system of equations should involve the leaving twelve singular points of φ who form a rational family $\mathcal{F}$ over $\mathbb{Q}(\mathcal{H})$:

$$\mathcal{F} = \{A, B, C, D, G, H, I, J, W, X, Y, Z\}$$

Using the π-adic developments, one pre-computes the values:

$$\left(\sigma_{\mathcal{F},1}(f^i g^j)\right)_{0\leq i+j\leq 4},\ \sigma_{\mathcal{F},1}(g),\ \sigma_{\mathcal{F},2}(g),\ \sigma_{\mathcal{F},3}(g) \in \mathbb{Q}(T)$$

By specializing, we obtain two new equations:

$$\sigma_{\mathcal{F},1}(\varphi) = 0, \quad \text{and} \quad \sigma_{\mathcal{F},1}(f\varphi) = 0,$$

Last, eliminating f in the two algebraic relations of $\frac{d\varphi}{d\omega} = 0$ and $P(f, g) = 0$, gives a degree twelve polynomial in g, whose zeros are the values of g at the twelve points of $\mathcal{F}$. Due to the pre-computation, coefficients in g^{11}, g^{10}, g^9 are known; this completes the system. We note that the two last equations are respectively quadratic and cubic while all the other are linear. So we need to use Groebner basis algorithm but the system is easily solved.

3.3 The p-adic deformation

In fact, all the previous computations were made modulo the prime $p = 11287$. We choose this prime because it splits completely in the compositum of the fields of definition of the singular points of φ. All the coefficients that appear belong to the *prime field* $\mathbb{F}_{11287}$ (and not in any extension of it).

We then have to recover the solution over $\mathbb{Q}$ from the one modulo p. To this end, we point out that all the complexity of our situation is contained in the divisor equality:

$$\left(\frac{\varphi^3 + H(T_0)(\varphi + 1)}{f}\right) = 2\left(\frac{d\varphi}{d\omega}\right).$$

From this equality, we derive an algebraic system[2] involving the coefficients b_{ij} of the equation P in f, g and the coefficients c_{ij} who make φ be a function of f and g. In order to avoid multiple solutions, we should normalize the equation P with respect to f and g. We are allowed to change f by $c_3 f$ and g by $c_0 + c_1 f + c_2 g$, $c_i \in \bar{\mathbb{Q}}$. Only one of these choices satisfies an equation normalized as follows:

$$f^3 - f^2 g - f^2 + b_{11} fg + b_{10} f + b_{03} g^3 + b_{01} g + b_{00} = 0$$

(we denote the same way the "old" and "new" functions f and g). Then the p-adic deformation reduces to a Newton-Hensel iteration, the first term, i.e. the solution modulo p, being given by results from sections 3.1 and 3.2.

Having the solution modulo an (heuristically) large enough power of p, and using the LLL-algorithm, we end the computation by recognizing the corresponding rational solution (see section 5 for a complete example).

3.4 Reconstructing the universal family

Using chinese remainder theorem and the fact that we can compute all the specializations of $\varphi \in \mathbb{Q}(\mathcal{H})(\mathcal{E})$ we want to, we are able to finish the computation of the universal family, that is computing explicitly the function φ. We summarize the final result in the following proposition:

Proposition 9 *The total space $\mathcal{E}$ of the universal family is the genus one curve over $\mathbb{Q}(T)$ defined by the equation:*

$$\begin{aligned}
0 = {} & f^3 - f^2 g - f^2 + \frac{1561T^4+5724T^3+6102T^2+2268T+729}{2220T^4+9072T^3+8424T^2+3888T+972} fg + \frac{36349T^5+105285T^4+93474T^3+72090T^2+22113T+6561}{102675T^5+407925T^4+373950T^3+247050T^2+78975T+18225} f \\
& + \frac{49729T^6+236826T^5+366255T^4+236844T^3+121743T^2+30618T+6561}{330750T^6+1628100T^5+2398410T^4+1697112T^3+747954T^2+236196T+39366} g^3 \\
& + \frac{-99458T^6-473652T^5-732510T^4-473688T^3-243486T^2-61236T-13122}{1540125T^6+7042950T^5+9280575T^4+7071300T^3+3408075T^2+984150T+164025} g \\
& + \frac{-2784824T^8+5833680T^7+66850416T^6+110327184T^5+57760128T^4+27981936T^3+2624400T^2+314928T-472392}{170953875T^8+1275223500T^7+3281715000T^6+3863335500T^5+3121395750T^4+1643530500T^3+629856000T^2+147622500T+22143375}
\end{aligned}$$

The function $\varphi : \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}(T)}$ that defines a degree 9 cover with monodromy $\mathbf{G}$*, ramified over the roots of $X^3 + H(T)(X + 1)$, ∞ with ramification type* $\mathbf{C}$ *is such that:*

$$\varphi = c_{21} f^2 g + c_{20} f^2 + c_{12} f g^2 + c_{11} fg + c_{10} f + c_{03} g^3 + c_{02} g^2 + c_{01} g + c_{00}$$

where the coefficients $c_{ij} \in \mathbb{Q}(T)$ can be download from:

`http://www.univ-tlse2.fr/grimm/algo/hallouin/PSL_2_F_8.result`.

[2] Groebner basis methods failed to solve such a system otherwise we would not bother developing the deformation method used here.

Here are the heights in T of the coefficients c_{ij}:

	c_{21}	c_{20}	c_{12}	c_{11}	c_{10}	c_{03}	c_{02}	c_{01}	c_{00}
height	19	18	13	16	15	13	11	13	12

Let us end this section by a:

Question — Is the genus one curve $\mathcal{E}$ over $\mathbb{Q}(T)$ an elliptic one?

4 Computation of the Hurwitz space $\mathcal{H}_{\mathbf{G}}$

In order to find specializations whose arithmetic and geometric Galois group are equal, we have to explicitly compute the cover $\mathcal{H}_{\mathbf{G}} \to \mathcal{H}$. It is known to be cyclic of degree 3. Thanks to Kummer theory, over $\mathbb{Q}(j)$ (with $j^2+j+1=0$), the corresponding field extension is a radical one which is parametrized by an element $a(T) \in \mathbb{Q}(j)(T)^*/\mathbb{Q}(j)(T)^{*3}$.

Thanks to the braid action, we verify that this cover is totally ramified over the two roots r, r' of $T^2+\frac{6}{49}T+\frac{9}{49}$. Therefore, there exists a constant $\gamma \in \mathbb{Q}(j)$ such that:

$$a(T) \equiv \gamma(T-r)^{\pm 1}(T-r')^{\pm 1} \pmod{\mathbb{Q}(j)(T)^{*3}}.$$

Moreover, because the descent to $\mathbb{Q}$ is possible, we have:

$$a(T) \equiv \gamma\frac{T-r}{T-r'} \pmod{\mathbb{Q}(j)(T)^{*3}} \qquad \text{and} \qquad N_{\mathbb{Q}(j)/\mathbb{Q}}(\gamma) \in \mathbb{Q}^{*3}.$$

The topology do not help anymore to find the constant γ because of its arithmetic nature. To find this constant γ, it suffices to compute the image of $a(T)$ by any specialization $\mathrm{ev}_{T_0} : \mathbb{Q}(j)(T)^*/\mathbb{Q}(j)(T)^{*3} \to \mathbb{Q}(j,T_0)^*/\mathbb{Q}(j,T_0)^{*3}$ where $T_0 \in \mathbb{C}$. We choose $T_0 = \frac{1}{2}$ and put:

$$\alpha = \mathrm{ev}_{T_0}(a) = \gamma\frac{\frac{1}{2}-r}{\frac{1}{2}-r'} \in \mathbb{Q}(j).$$

One can relate α to the specialized cover $\varphi : \mathcal{E}_{\frac{1}{2}} \to \mathbb{P}^1_{\mathbb{Q}}$, or more precisely to $\mathcal{E}^{\mathrm{gal}}_{\frac{1}{2}} \to \mathbb{P}^1_{\mathbb{Q}}$ its Galois closure . Indeed, the constant field of $\mathbb{Q}(\mathcal{E}^{\mathrm{gal}}_{\frac{1}{2}})$ is a degree 3 cyclic extension k of $\mathbb{Q}$, $\mathrm{Gal}(k/\mathbb{Q}) = \langle\sigma\rangle$, and α corresponds to $k(j)/\mathbb{Q}(j)$ by Kummer theory:

$$k(j) = \mathbb{Q}(j)(\sqrt[3]{\alpha}).$$

We find that the extension $k/\mathbb{Q}$ is the unique cubic extension of discriminant 79^2:

$$\begin{cases} k = \mathbb{Q}(\theta) \\ \theta^3-\theta^2-32\theta+79=0 \end{cases} \quad \Longrightarrow \quad \begin{cases} k(j) = \mathbb{Q}(j)\left(\sqrt[3]{\beta}\right) \\ \beta = (\theta + j^2\sigma(\theta) + j\sigma^2(\theta))^3 \in \mathbb{Q}(j). \end{cases}$$

Kummer theory again shows that $\alpha = \beta$ or β^2; this completes the computation of the element $a(T)$.

Over $\mathbb{Q}(j)$, in term of fields extension, the cover $\mathcal{H}_{\mathbf{G}} \to \mathcal{H}$ is given by:

$$\mathbb{Q}(j,T) \subset \mathbb{Q}(j,T)(\sqrt[3]{a(T)})$$

The descent to $\mathbb{Q}$ is easy: the element $\sqrt[3]{a(T)}+\frac{(N_{\mathbb{Q}(j)/\mathbb{Q}}(\gamma))^{1/3}}{\sqrt[3]{a(T)}}$ is algebraic over $\mathbb{Q}(T)$ and has the following minimal polynomial:

$$X^3 - 3N_{\mathbb{Q}(j)/\mathbb{Q}}(\gamma)^{1/3}X - \frac{\mathrm{Tr}_{\mathbb{Q}(j)/\mathbb{Q}}(\gamma)T^2 - 2\,\mathrm{Tr}_{\mathbb{Q}(j)/\mathbb{Q}}(\gamma r)T + \mathrm{Tr}_{\mathbb{Q}(j)/\mathbb{Q}}(\gamma r^2)}{(T-r)(T-r')} \in \mathbb{Q}(T)[X].$$

With the help of `magma`, we compute a parameter S of this curve and deduce that:

Proposition 10 *The cover $\mathcal{H}_{\mathbf{G}} \to \mathcal{H}$ is given by the rational fraction $T = H_G(S)$ with:*

$$H_G(S) - \frac{1}{49} = -\frac{2^3 \times 43 \times 419 \times (S-\frac{121588}{441})(S-\frac{67537}{441})}{3 \times 7^3 \times (S^3 - 582S^2 + \frac{721028699}{9261}S - \frac{294590157121}{12252303})}. \tag{5}$$

This expression points out the value $T = \frac{1}{49}$ over which there are three rational points. Finding other such values is now easy:

Proposition 11 *The positive values of T over which there are three rational points in the cover $\mathcal{H}_{\mathbf{G}} = \mathbb{P}^1_{\mathbb{Q},S} \to \mathcal{H} = \mathbb{P}^1_{\mathbb{Q},T}$ and whose numerator and denominator have less than three digits are:*

$$\left\{ \tfrac{489}{41}, \tfrac{1}{49}, \tfrac{17}{113}, \tfrac{703}{127}, \tfrac{51}{211}, \tfrac{971}{251}, \tfrac{109}{349}, \tfrac{197}{533}, \tfrac{57}{617}, \tfrac{321}{769} \right\}.$$

All these values correspond to covers in our family who have arithmetic and geometric Galois groups equal to $PSL_2(\mathbb{F}_8)$.

5 Two numerical examples: the values $T = \frac{1}{49}$ and $T = \frac{1}{2}$

In this section, we conveniently specialize the preceding results in order to compute totally real polynomials over $\mathbb{Q}$ with Galois group equal to $PSL_2(\mathbb{F}_8)$ or $P\Gamma L_2(\mathbb{F}_8)$.

Due to formula (5), there are three rational points $S = \infty$, $\frac{121588}{441}$, $\frac{67537}{441}$ above the value $T = \frac{1}{49}$; this means that the cover $\varphi : \mathcal{E}_{\frac{1}{49}} \to \mathbb{P}^1_{\mathbb{Q}}$ has geometric and arithmetic Galois groups equal to $PSL_2(\mathbb{F}_8)$. By specializing results from §3, one computes the equation between (the specializations of) f and g:

$$f^3 - f^2 g - f^2 + \tfrac{68425}{92796} fg + \tfrac{9714395}{27506688} f + \tfrac{382202500}{2350284363} g^3 - \tfrac{3822025}{48996288} g - \tfrac{230085905}{12594624768} = 0$$

and the function $\varphi \in \mathbb{Q}(f, g)$:

$$\varphi = \tfrac{14303337369036758568345 6}{6840410226716265675875} f^2 g - \tfrac{38163798107779728384}{7347379405710274625} f^2 - \tfrac{7876734306017280}{357946911740047} fg^2 + \tfrac{245154404440349184}{99969458921684555} fg + \tfrac{23639734871190207}{3758250335401675} f + \tfrac{2625578102005760}{357946911740047} g^3 + \tfrac{8063814809600}{2484834242989} g^2 - \tfrac{35024389280012}{36525195075515} g - \tfrac{17895514803768}{9611893440925}.$$

Using proposition 4, we know that all the singular values of φ are real; let $\lambda_2 > \lambda_3$ denote the two negative ones. Then $]\lambda_3, \lambda_2[$ is an interval of totally real specialization and it contains the rational $-\frac{3}{2}$. Specializing the cover $\varphi : \mathcal{E}_{\frac{1}{49}} \to \mathbb{P}^1_{\mathbb{Q}}$ at $\varphi = -\frac{3}{2}$ gives rise to:

Proposition 12 *Over $\varphi = -\frac{3}{2}$, the cover $\varphi : \mathcal{E}_{\frac{1}{49}} \to \mathbb{P}^1_{\mathbb{Q}}$ specializes to the $\mathbb{Q}$-extension defined by the following polynomial:*

$$\begin{aligned} &x^9 - 4x^8 - 23908787388x^7 - 759515260327432x^6 + 1580037311850766399 33x^5 + 952261161378623989643982 0x^4 \\ &- 827738782216529877093838210 92x^3 - 167307009896512243981112148712743 84x^2 \\ &- 383866034575302084802931793638509630716x - 263692091645532308205828937593259228110772 8 ; \end{aligned}$$

it is a totally real polynomial which has Galois group equal to $PSL_2(\mathbb{F}_8)$.

On the other hand, if we choose $T = \frac{1}{2}$, the cover $\varphi : \mathcal{E}_{\frac{1}{2}} \to \mathbb{P}^1_{\mathbb{Q}}$ has a geometric Galois group equal to $PSL_2(\mathbb{F}_8)$ while its arithmetic one is equal to $P\Gamma L_2(\mathbb{F}_8)$. Over $\varphi = -\frac{3}{2}$, one now has:

Proposition 13 *Over $\varphi = -\frac{3}{2}$, the cover $\varphi : \mathcal{E}_{\frac{1}{2}} \to \mathbb{P}^1_{\mathbb{Q}}$ specializes to the $\mathbb{Q}$-extension defined by the following polynomial:*

$$\begin{aligned} &x^9 + 3x^8 - 3553997352x^7 - 4298221687088x^6 + 30530754907898176 54x^5 + 1383921342510140116965 8x^4 \\ &- 68371655160088535001851440 0x^3 - 61550721923867455822882342803 12x^2 \\ &- 60075422489715651961994506176566 87x - 14227396806201099187283927015663906 77 ; \end{aligned}$$

it is a totally real polynomial which has Galois group equal to $P\Gamma L_2(\mathbb{F}_8)$.

References

[Cou99] Jean-Marc Couveignes. Tools for the computation of families of coverings. In Helmut Vlkein, David Harbater, Peter Mller, and J.G. Thompson, editors, *Aspects of Galois theory*, volume 256 of *London Mathematical Society Lecture Note Series*, pages 38–65. Cambridge, 1999. The following pages of this book were inadvertently numbered incorrectly: p. 21 should be p. 22, p. 22 should be p. 23 and p. 23 should be p. 21.

[Cou00] Jean-Marc Couveignes. Boundary of hurwitz spaces and explicit patching. *Journal of Symbolic Computation*, 30:739–759, 2000.

[Det04] Michael Dettweiler. Plane curve complements and curves on hurwitz spaces. *J. Reine Angew. Math.*, 573:19–43, 2004.

[DF94] Pierre Dbes and Michael D. Fried. Nonrigid constructions in galois theory. *Pacific Journal of Mathematics*, 163(1):81–122, 1994.

[Fri95] Michael D. Fried. Introduction to modular towers. In Shreeram S. Abhyankar, Walter Feit, Yasutaka Ihara, and Helmut Vlklein, editors, *Recent Developments in the Inverse Galois Problem*, volume 186 of *Contemporary Mathematics*, pages 111–171. American Mathematical Society, 1995.

[FV91] Michael D. Fried and Helmut Vlklein. The inverse galois problem and rational points on moduli spaces. *Mathematische Annalen*, 290:771–800, 1991.

[HRD03] Emmanuel Hallouin and Emmanuel Riboulet-Deyris. Computation of some moduli spaces of covers and explicit s_n and a_n regular $\mathbb{Q}(t)$-extensions with totally real fibers. *Pacific Journal of Mathematics*, 211(1):81–99, 2003.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford, 2002.

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer, 1999.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.

[Vl96] Helmut Vlklein. *Groups as Galois Groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge, 1996.

[Wew98] Stefan Wewers. *Construction of Hurwitz spaces*. PhD thesis, Universitt-Gesamthochschule, Essen, 1998.